UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF ONE APPLE IPHONE, SERIAL NUMBER F4GV8GUNJC6F	APPLICATION FOR A SEARCH WARRANT FOR AN ELECTRONIC DEVICE Case No. 18-M-1009

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Melissa Galicia, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I have been a Special Agent with the Federal Bureau of Investigation ("FBI") for more than four years. During my tenure with the FBI, I have participated in investigations involving, among other things, fraud and financial crimes. I have also conducted interviews, made arrests, executed search warrants, and secured other relevant information using a variety of investigative techniques. I am familiar with the facts and circumstances set forth below from my participation in the investigation; my review of the investigative file; my communication with other law enforcement officers; my review of reports of other law enforcement officers involved in the investigation; and my review of other records associated with the investigation.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The information contained in this affidavit includes information that I obtained from other law enforcement agents and officers, and from law enforcement and public records databases. The statements described in this affidavit are set forth in sum, substance, and in part.

THE SUBJECT DEVICE AND PRIOR APPLICATION

4. This affidavit is submitted in support of an application for a warrant to search: ONE APPLE IPHONE, SERIAL NUMBER F4GV8GUNJC6F (the "SUBJECT DEVICE"), which is currently within the possession of the FBI within the Eastern District of New York, described in Attachment A, for evidence, instrumentalities, contraband and/or fruits of violations of federal criminal law, including Theft Concerning Programs Receiving Federal Funds, in violation of 18 U.S.C. Section 666(a)(1)(A), and Health Care Fraud, in violation of 18 U.S.C. Section 1347 (the "SUBJECT OFFENSES").

8. On October 2, 2018, the Honorable Vera M. Scanlon, United States Magistrate Judge for the Eastern District of New York, signed a complaint and issued arrest warrants authorizing the arrest of several defendants, including MARINA GOLFO ("GOLFO"), and charging them with the SUBJECT OFFENSES, see United States v. Doyle et al., 18 MJ 927 (the "Complaint"). The Complaint is attached hereto as Exhibit A and incorporated herein by reference.

9. On October 4, 2018, agents from the FBI and DOI arrested GOLFO and seized the SUBJECT DEVICE incident to that arrest. Specifically, law enforcement agents

seized the SUBJECT DEVICE from GOLFO's bedroom, after observing the phone on GOLFO's nightstand.

10. On or about October 19, 2018, the Honorable Cheryl L. Pollack, United States Magistrate Judge for the Eastern District of New York, signed a search warrant authorizing the search of the SUBJECT DEVICE from the time period August 1, 2012 through April 30, 2018 (the "October 19, 2018 search warrant"). A copy of the October 19, 2018 search warrant is attached hereto as Exhibit B and incorporated herein by reference.

11. Since the issuance of the October 19, 2018 search warrant, law enforcement agents have gathered additional evidence, described in more detail below, reflecting that GOLFO continued to commit the SUBJECT OFFENSES after April 30, 2018 and up to the date of her arrest, October 4, 2018. Accordingly, the government is now seeking authorization to search the SUBJECT DEVICE, which is already in the possession of the FBI, for evidence, fruits and instrumentalities of the SUBJECT OFFENSES for the time period May 1, 2018 through October 4, 2018.

PROBABLE CAUSE

A. Background

5. As set forth in the Complaint, the FBI and the New York City Department of Investigation ("DOI") have been conducting an investigation into allegations of fraudulent billing practices in connection with the New York State Early Intervention Program (the "EIP"), a program that provides remedial services to developmentally delayed children from birth to age three. Such services may include physical, occupational, and speech therapy; special instruction; and social work services. These services are provided by individual

therapists who are either subcontractors or employees of agencies that hold EIP contracts with the New York State Department of Health ("NYS DOH"). NYC DOHMH administers the EIP in New York City and conducts audit, quality assurance, and compliance oversight of the Ell), under the ultimate oversight of NYS DOH.

6. In order to receive payment for an EIP therapy session, a therapist must provide a written report, known as a session note, documenting his or her session with a child. Sessions generally occur in half-hour or one-hour increments. These session notes detail the date, time and place of the session as well as some details of the therapy given and the child's progress in response to the treatment. Session notes must be signed by the therapist and the parent or guardian of the child immediately after the EIP therapy session ends.

12. As set forth in the Complaint, the investigation initially revealed that in or about and between April 2015 and February 2018, GOLFO, an EIP therapist, submitted numerous fraudulent session notes and accompanying invoices for non-existent EIP sessions purportedly occurring in the Eastern District of New York and elsewhere.

B. The Prior Search of the Subject Device

13. Pursuant to the October 19, 2018 search warrant, law enforcement agents reviewed the SUBJECT DEVICE and found evidence of the SUBJECT OFFENSES. Specifically, throughout the time period charged in the indictment, GOLFO took numerous geotagged photographs that revealed that, even though she billed for an EIP session occurring at a certain date, time and location, she was not at that session location and was not performing a session at that time.

14. For example, on November 27, 2017, GOLFO's phone was used to take a photograph depicting a banner for a rock band; the geotagged location for this photograph was in the Midtown neighborhood of Manhattan. Internet research revealed that this particular rock band performed a concert on that date at a music venue located in the Midtown neighborhood of Manhattan. At the same time that this photograph was taken, GOLFO claimed in a session note to have performed a therapy session with a child purportedly occurring in the Bronx.

15. Similarly, on October 14, 2017, GOLFO's phone was used to take a photograph of GOLFO appearing in front of a lake; the geotagged location for this photograph was in the vicinity of the North-South Lake Campground, located in upstate New York. At the same time that this photograph was taken, GOLFO claimed in a session note to have performed a therapy session with a child located in New York City, approximately 120 miles from the North-South Lake Campground.

C. Additional Evidence of Fraud

16. Following the issuance of the October 19, 2018 search warrant, law enforcement agents gathered additional evidence reflecting that GOLFO continued to commit the charged offenses after April 30, 2018 and up to the date of her arrest, October 4, 2018.

17. Specifically, law enforcement officers reviewed GOLFO's session notes for the time period January 11, 2018 through September 2018 and determined that, during that time period, the defendant submitted session notes for therapy sessions for only one child,

purporting to provide this child with twenty hours of therapy sessions per week – four hours of service per day, five days per week. Law enforcement officers thereafter contacted the parent and grandparent for the relevant child and learned that GOLFO was not providing twenty hours of service per week during this time period. According to the parent and grandparent of the child, GOLFO provided no more than one hour of service per week to the child during this time period, resulting in at least nineteen hours of fraudulently billed therapy sessions per week between January 2018 and September 2018.

18. In addition, law enforcement officers conducted surveillance on the child's home on May 10, 2018 and May 11, 2018. On those dates, law enforcement officers did not observe GOLFO or any of her vehicles in the vicinity of the child's home, however they did observe one of GOLFO's vehicles parked in the vicinity of GOLFO's personal residence. GOLFO subsequently submitted session notes in which she fraudulently claimed to have provided four hours of therapy on each of those dates at the child's home during the time periods that law enforcement officers conducted surveillance.

19. On or about February 22, 2019, a grand jury in the Eastern District of New York returned an indictment charging GOLFO with one count of theft of funds, in violation of 18 U.S.C. § 666(a)(1)(A) and one count of health care fraud, in violation of 18 U.S.C. § 1347(a), for the aforementioned conduct between April 2015 and September 2018. A copy of the indictment is attached hereto and incorporated by reference.

20. Based on the foregoing, there is probable cause to believe that there is information on the SUBJECT DEVICE concerning the SUBJECT OFFENSES from the time period May 1, 2018 through October 4, 2018.

TECHNICAL TERMS

20. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or

locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also

include global positioning system ("GPS") technology for determining the location of the device.

f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

21. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, PDA, to take, store and share photographs and videos and use a variety of apps. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

22. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

23. As further described in Attachment B, this application seeks permission to locate not only data that might serve as direct evidence of the SUBJECT OFFENSES, but also for forensic electronic evidence that establishes how the SUBJECT DEVICE was used, the purpose of its use, who used it and when. There is probable cause to believe that this forensic electronic evidence can be recovered from the SUBJECT DEVICE because:

a. Data on an electronic device can provide evidence of a file that was once on the device but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file.)

b. Forensic evidence on an electronic device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works can, after examining this forensic evidence in its proper context, draw conclusions about how devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs or other forms of forensic evidence on an electronic device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, such evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on an electronic device is evidence may depend on other information stored on the device and the application of knowledge about how the device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding user attribution evidence, sometimes it is necessary to establish that a particular thing is not present on an electronic device. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

24. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the SUBJECT DEVICE consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the SUBJECT DEVICE to human inspection in order to determine whether it is evidence described by the warrant.

25. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not

involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

26. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the SUBJECT DEVICE described in Attachment A to seek the items described in Attachment B, which items constitute instrumentalities, fruits and evidence of violations of Title 18, United States Code, Sections 666(a)(1)(A) and 1347.

Respectfully submitted,

MELISSA GALICIA
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on January 8, 2020:

THE HONORABLE SANKET J. BULSARA
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

The property to be searched is ONE APPLE IPHONE, SERIAL NUMBER F4GV8GUNJC6F (the "SUBJECT DEVICE"), hereinafter the "Device." The Device is currently located in FBI custody in the Eastern District of New York. This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

27. All records on the SUBJECT DEVICE described in Attachment A that relate to violations of Title 18, United States Code, Sections 666(a)(1)(A) and 1347 and involve MARINA GOLFO from the period May 1, 2018 through October 4, 2018, including:

a. names and telephone numbers, as well as the contents of all call logs, contact lists, text messages (including iMessages and messages contained in messaging applications), emails (including those sent, received, deleted and drafted), instant messages, photographs, videos, social media posts and/or messages, Internet activity (including browser history, web page logs, and search terms entered by the user), geo-location data, application data, and other electronic media;

b. evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as, for example, logs, phonebooks, saved usernames and passwords, documents, and browsing history;

c. evidence of software that would allow others to control the Device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software; .

d. evidence of the times the Device was used;

e. passwords, encryption keys, and other access devices that may be necessary to access the Device; and

f. contextual information necessary to understand the evidence described in this Attachment.

All of which constitute fruits or instrumentalities of violations of Title 18, United States Code, Sections 666(a)(1)(A) and 1347.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.